

# **EXHIBIT**

# **K**

01/19/2008 17:30 FAX

003/018

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California  
Corporation,

Plaintiff and  
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a  
Delaware corporation, INTERNET  
SECURITY SYSTEMS, INC., a Georgia  
Corporation, and SYMANTEC  
CORPORATION, a Delaware corporation,

Defendants and  
Counterclaim-Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

**SYMANTEC CORPORATION'S FOURTH SUPPLEMENTAL RESPONSE TO SRI  
INTERNATIONAL, INC.'S INTERROGATORY NO. 6**

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendant Symantec Corporation ("Symantec") supplements its responses to Plaintiff SRI International, Inc.'s ("SRI") Interrogatory No. 6.

**GENERAL RESPONSES**

1. Symantec's responses to SRI's First Set of Interrogatories are made to the best of Symantec's present knowledge, information and belief. Symantec's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. Symantec undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2. Symantec's responses to SRI's First Set of Interrogatories are made according to

01/18/2008 17:30 FAX

004/018

information currently in Symantec's possession, custody and control.

3. To the extent that Symantec responds to SRI's First Set of Interrogatories by stating information that is private, business confidential, proprietary, trade secret or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7) or Federal Rule of Evidence 501, Symantec will respond pursuant to the terms of the Protective Order in this case.

4. Symantec reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility of any information, document or thing produced in response to SRI's Interrogatories as evidence in any subsequent proceeding or trial in this or any other action for any purpose whatsoever.

5. Symantec reserves the right to object on any ground at any time to additional interrogatories that SRI may propound involving or relating to the same subject matter as SRI's First Set of Interrogatories.

#### **OBJECTIONS**

Symantec incorporates the Objections contained in Symantec's Response to SRI's First Set of Interrogatories. The applicable foregoing general objections are incorporated into each of the specific objections and responses that follow. The stating of a specific objection or response shall not be construed as a waiver of Symantec's general objections.

#### **THIRD SUPPLEMENTAL RESPONSE TO PLAINTIFF'S INTERROGATORY NO. 6**

##### **INTERROGATORY NO. 6:**

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific statutory bases for the invalidity (e.g., 35 U.S.C. § 102(a)), the factual bases for that contention, any allegedly invalidating prior art or publications, where each element of the claim is found in

01/18/2006 17:30 FAX

005/016

the prior art or publications, and the three people most knowledgeable about the factual bases for your contention. Your response may take the form of a claim chart.

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:**

Symantec objects to Interrogatory No. 6 to the extent that it requests the "three people most knowledgeable about the factual bases for your contentions." This portion of the interrogatory seeks the premature identification of the expert witnesses upon which Symantec intends to rely. Symantec further objects that this Interrogatory is overbroad to the extent that it requests information regarding claims that SRI has not asserted against Symantec in this litigation. SRI provided Symantec with a list of claims-at-issue in the Sept. 27, 2005 letter from Gina M. Steele to Jonathan D. Loeb.<sup>1</sup> However, SRI later asserted additional claims in its "Second Supplemental Responses to Defendant Symantec's First Set of Interrogatories [Nos. 1-12]," received by Symantec on November 21, 2005.<sup>2</sup> The addition of these claims at such a late date is prejudicial to Symantec. To the extent that SRI may later try to assert still more additional claims against Symantec, such action by SRI would again be highly prejudicial to Symantec. Symantec reserves the right to supplement or modify these responses should SRI belatedly add additional claims.

Symantec has not yet had an opportunity to explore through discovery the factual

---

<sup>1</sup> SRI's Sept. 27, 2005 letter stated: "Interrogatory No. 1. With regard to your request for the claims SRI is asserting against Symantec, SRI states as follows: SRI asserts that Symantec has infringed claims 1-23 of the '615 patent; claims 1-18, and 20-24 of the '212 patent; claims 1-5, 8-16, 18-22 of the '203 patent; and claims 1, 4, 11-18, 21 and 24 of the '338 patent."

<sup>2</sup> Specifically, claims 2, 3, 5-8, 10, 19, and 25 of the '338 patent, claims 6, 7, and 17 of the '203 patent, claim 19 of the '212 patent, and claims 34-43, 44-53, 64-73, and 84-93 were all belatedly asserted against Symantec in SRI's "Second Supplemental Responses to Defendant Symantec's First Set of Interrogatories [Nos. 1-12]." These claims, together with the claims identified in SRI's Sept. 27, 2005 letter, will be referred to herein as "the claims-at-issue."

01/19/2006 17:31 FAX

008/016

predicates underlying SRI's claimed conception dates for the alleged inventions. Consequently, the patentability of the claims-at-issue must be assessed in light of the state of the relevant art as of the filing date of the original application from which the patents issued. Symantec intends to present evidence at trial that establishes and broadly illustrates the state of the art in intrusion detection and network monitoring on or before November 9, 1998. Symantec may rely upon publications, patents, percipient and expert testimony, and/or contemporaneous and predecessor products to reveal the state of such art at that time (or as of any earlier date if Plaintiff offers legally adequate proof of an earlier date of invention).

The information provided in Symantec's response is preliminary in nature and subject to modification and supplementation. For example, Symantec has only recently received limited documents from SRI relating to the development work that led to the patents-in-suit and certain prior art systems and references, which Symantec has begun to review. Symantec has not yet had an opportunity to depose the individuals involved in the conception and reduction-to-practice of the alleged inventions. Symantec continues to develop and refine its understanding of the state of the art as additional relevant information is acquired during the course of ongoing discovery. Ongoing discovery efforts may identify additional prior art references or embodiments that are relevant to the invalidity of the claims-in-suit. Symantec will supplement this response in a timely manner upon receipt of sufficient information relating to such additional prior art references or embodiments.

Symantec further objects that this interrogatory is premature because Symantec has not been provided with any understanding of SRI's proposed claim constructions, and therefore is unable to determine how SRI's proposed claim constructions inform the anticipation and

01/18/2006 17:31 FAX

007/018

obviousness contentions disclosed herein. Furthermore, the contentions set forth below are not based upon Symantec's proposed claim constructions. Symantec reserves the right to supplement and modify its invalidity contentions under 35 U.S.C. §§ 102 and 103 subject to the claim constructions advanced by SRI and Symantec pursuant to the Court's Scheduling Order, which specifies that "on January 20, 2006, the parties shall exchange lists of those claim terms that they believe need construction and their proposed claim construction of those terms" and that the "parties shall agree upon and file the Joint Claim Construction Statement on February 17, 2006, with the claim chart separately docketed." The complete scope of available prior art and its applicability to individual claims-at-issue will not be certain until the Court has construed the claims of the patents-in-suit. Symantec therefore further reserves the right to supplement and modify these contentions once the Court has construed the claims.

The accompanying prior art charts, attached hereto as Exhibits A-1 – A-23, reflect Symantec's current understanding of the primary prior art references and embodiments upon which it intends to rely to establish anticipation of the claims-in-suit under 35 U.S.C. § 102 and/or obviousness under 35 U.S.C. § 103. To the extent that a particular prior art reference or embodiment does not alone anticipate all the limitations of any one of the claims-in-suit as ultimately construed by the court, Symantec reserves the right to combine the references and/or embodiments disclosed herein with other references and/or embodiments that may complement any such reference or embodiment, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Moreover, due to the extremely large number of prior art references that invalidate the claims at issue, Symantec cannot possibly list every combination of art that renders the claims-at-issue invalid under 35 U.S.C. § 103, and reserves the right to present different combinations of

01/19/2006 17:31 FAX

008/016

references and/or embodiments, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

#### **Relevant Prior Art References Identified To Date**

The knowledge of one skilled in the art as of Nov. 9, 1998 would have been informed by access to and appreciation of at least the following practices, publications, patents, and publicly available technologies, products, and systems. Symantec intends to rely upon these and similar references to establish the state of the anomaly detection, intrusion detection, network monitoring, and related arts on or before Nov. 9, 1998, and to establish that the claims-in-suit were anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 on or before Nov. 9, 1998:

- All prior art of record in the file histories of the patents-in-suit; or identified in the Background of the Invention section of the patents-in-suit;
- All prior art references identified in Exhibits A-1 – A-23 attached hereto; and
- All prior art references produced to SRI at Bates ranges SYM\_P\_0067248 – SYM\_P\_0082535; SYM\_P\_0499257 – SYM\_P\_0506549; SYM\_P\_0511902 – SYM\_P\_0513006; SYM\_P\_0526260 – SYM\_P\_0531122; SYM\_P\_0531123 – SYM\_P\_0531139; SYM\_P\_0534104 – SYM\_P\_0534116; SYM\_P\_0535194 – SYM\_P\_0535341.

#### **Additional Technologies, Products and Systems**

- Argus,
- Arpwatch,
- ASIM (Automated Security Incident Measurement),
- Berkeley Packet Filter,
- Borderguard,
- Bro,
- Cabletron's Spectrum,
- CIDF (Common Intrusion Detection Framework),
- Computer Associates Unicenter TNG,
- CSM (Cooperating Security Managers),
- DIDS (Distributed Intrusion Detection System),

01/18/2008 17:31 FAX

009/018

- EMERALD,
- FireWall-1,
- GrIDS (Graph based Intrusion Detection System),
- Harris Corporation Stake Out,
- Haystack,
- HP OpenView, Network Node Manager, and NetMetrix,
- IDES,
- Internet standards,
- IP Filter,
- ISM (Internetwork Security Manager),
- Ji-Nao,
- Libpcap,
- MIDAS (Multics Intrusion Detection and Alerting System),
- NADIR (Network Anomaly Detection and Intrusion Reporter),
- NetRanger,
- NFR (Network Flight Recorder),
- NIDES,
- NIDX,
- NSM (Network Security Monitor),
- Raxco AUDIT,
- Stalker, NetStalker and WebStalker,
- Sun Network Management System (Solstice Site Manager, Solstice Domain Manager, Solstice Enterprise Manager, and Sun Net Manager),
- SunScreen,
- Topdump,
- TCP Wrapper,
- TIS Firewall Toolkit,
- Tivoli Enterprise Manager, and
- Wisdom & Sense.

01/18/2006 17:31 FAX

010/016

**PRIOR ART REFERENCES THAT ANTICIPATE THE ASSERTED CLAIMS-  
AT-ISSUE**

The prior art cited herein invalidates the claims at issue under 35 U.S.C. §102, as set forth in detail in the representative charts attached as Exhibits A-1 – A-22 to this Supplemental Response. The cover page of each chart provides citations to referenced prior art, as well as citations to related prior art disclosures. Representative anticipatory references include:

- Exhibit A-1: "Emerald 1997" and the additional references listed on page 1 of Exhibit A-1;
- Exhibit A-2: "Emerald - CMAD" and the additional references listed on pages 1-2 of Exhibit A-2;
- Exhibit A-3: "Emerald - Conceptual Overview" and the additional references listed on pages 1-2 of Exhibit A-3;
- Exhibit A-4: "Emerald - Conceptual Design 1997" and the additional references listed on pages 1-2 of Exhibit A-4;
- Exhibit A-5: "Emerald - Live Traffic Analysis" and the additional references listed on page 1 of Exhibit A-5;
- Exhibit A-6: "Network NIDES" and the additional references listed on page 1 of Exhibit A-6;
- Exhibit A-7: "Ji-Nao" (includes "Ji-Nao" and "Ji-Nao slides") and the additional references listed on page 1 of Exhibit A-7;
- Exhibit A-8: "NSM" and the additional references listed on page 1 of Exhibit A-8;
- Exhibit A-9: "DIDS February 1991 and DIDS October 1991" and the additional references listed on pages 1-2 of Exhibit A-9;
- Exhibit A-10: "Grids 1996 and Grids 1997" and the additional references listed on page 1 of Exhibit A-10;
- Exhibit A-11: "NetRanger" (includes "NetRanger User Guide 1.3.1" and "NetRanger product") and the additional references listed on pages 1-2 of Exhibit A-11;
- Exhibit A-12: "RealSecure" and the additional references listed on page 1 of Exhibit A-12;
- Exhibit A-13: "Network Level Intrusion Detection;"
- Exhibit A-14: "U.S. Pat. No. 5,825,750" and the additional reference listed on page 1 of Exhibit A-14;
- Exhibit A-15: "Fault Detection in an Ethernet Network via anomaly detectors" and the additional references listed on page 1 of Exhibit A-15;

01/18/2008 17:32 FAX

011/018

- Exhibit A-16: "Stake Out Network Surveillance" and the additional reference listed on page 1 of Exhibit A-16;
- Exhibit A-17: "HP OpenView" and the additional references listed on pages 1-2 of Exhibit A-17;
- Exhibit A-18: "ISM" and the additional reference listed on page 1 of Exhibit A-18;
- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994;"
- Exhibit A-20: "Netstalker and HP OpenView" and the additional references listed on page 2 of Exhibit A-20;
- Exhibit A-21: "Network Flight Recorder" and the additional references listed on pages 1-2 of Exhibit A-21; AND
- Exhibit A-22: "AIS."

Citations to particular pages of a prior art reference in the attached prior art charts are to be understood as exemplary. Other pages of a prior art reference may also be relevant to the existence of a claim element, and Symantec reserves its right to supplement the page citations provided, if necessary. Symantec further reserves the right to supplement its § 102 contentions with additional prior art references because Symantec's investigation is still preliminary.

#### **PRIOR ART REFERENCES THAT RENDER THE CLAIMS-AT-ISSUE OBVIOUS**

In addition to anticipating the claims-at-issue, a very large number of combinations of the prior art references identified render some or all of the claims-at-issue obvious under 35 U.S.C. § 103. Representative examples of invalidating combinations of the prior art references are identified below. Symantec reserves the right to establish that any alleged "invention" claimed in the patents-in-suit would have been obvious and thus invalid under 35 U.S.C. § 103 based upon any combination of references identified herein, or similar to those identified herein, that one skilled in the art as of Nov. 9, 1998 would have had motivation to create.

- Exhibit A-2: "Emerald - CMAD" (for indicated claims);
- Exhibit A-3: "Emerald - Conceptual Overview" (for indicated claims);

01/19/2008 17:32 FAX

012/018

- Exhibit A-4: "Emerald - Conceptual Design 1997" (for indicated claims);
- Exhibit A-17: "HP OpenView" (see page 2 of Exhibit A-17 regarding § 103 combinations);
- Exhibit A-18: "ISM" (see page 1 of Exhibit A-18 regarding § 103 combinations);
- Exhibit A-19: "Emerald 1997, Intrusive Activity 1991, NIDES 1994" (see page 1 of Exhibit A-19 regarding § 103 combinations);
- Exhibit A-20: "NetStalker and HP OpenView" (see page 2 of Exhibit A-20 regarding § 103 combinations);
- Exhibit A-21: "Network Flight Recorder" (for indicated claims);
- Exhibit A-23: Summary chart of other relevant prior art, listing, for each individual limitation of each claim-at-issue, the prior art references that satisfy each limitation and could be combined with any of the references listed in Exhibits A-1 – A-22.

Symantec has provided as Exhibit A-23 a chart indicating prior art references disclosing particular limitations of each claim-at-issue. Given the large number of combinations, Symantec cannot identify all of the possible permutations at this time. For each of the prior art charts listed above for anticipation and/or obviousness, any missing claims or limitations could be satisfied by combining the cited reference of the prior art chart with reference(s) from Exhibit A-23.

Symantec reserves the right to combine the cited references in any combination or permutation that one of skill in the art as of Nov. 9, 1998 would have had motivation to create or evaluate. Symantec further reserves the right to supplement its § 103 contentions with additional prior art references because Symantec's investigation is still preliminary.

#### **THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112**

The claims-at-issue are also invalid for failure to satisfy the best mode requirement under 35 U.S.C. § 112. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of the source code provided in the Appendix indicates that the code in the Appendix is not the complete program that existed at the time. For example, the Appendix code would not compile and run. In addition, the Appendix code contains no configuration files

01/19/2006 17:32 FAX

013/018

allowing for the use of any particular network traffic data categories. Furthermore, the Appendix code does not appear to have code for a resolver or an expert system. On information and belief, Symantec believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventors' best mode of practicing the claims-at-issue.

In addition, the patents-in-suit are invalid for failure to satisfy the enablement and written description requirements of 35 U.S.C. § 112. Furthermore, the claims-at-issue are invalid as indefinite because the claims fail to particularly point out and distinctly claim the subject matter of the invention.

Symantec's contentions regarding the invalidity of SRI's patents-in-suit pursuant to 35 U.S.C. § 112 are preliminary and subject to modification and review. For example, Symantec has not yet had the opportunity to depose either of the inventors.

Dated: January 19, 2006

DAY CASEBEER  
MADRID & BATCHELDER LLP

By: Paul Grewal / HL  
Paul S. Grewal

Paul S. Grewal (*pro hac vice*)  
Day Casebeer Madrid & Batchelder LLP  
20300 Stevens Creek Blvd., Suite 400  
Cupertino, CA 95014  
Tel: (408) 873-0110  
Fax: (408) 873-0220

*Attorneys for Defendant and Counterclaim-  
Plaintiff Symantec Corporation*

01/18/2006 17:32 FAX

014/018

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)  
Robert M. Galvin (*pro hac vice*)  
Paul S. Grewal (*pro hac vice*)  
Day Casebeer Madrid & Batchelder LLP  
20300 Stevens Creek Blvd., Suite 400  
Cupertino, CA 95014  
Tel: (408) 873-0110  
Fax: (408) 873-0220

Michael J. Schallopp (*pro hac vice*)  
Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014  
Tel: (408) 517-8000  
Fax: (408) 517-8121

Dated: January 19, 2006

# EXHIBIT L

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,	)	
a California Corporation,	)	
	)	
Plaintiff and	)	
Counterclaim-Defendant,	)	
	)	
v.	)	
	)	C. A. No. 04-1199 (SLR)
INTERNET SECURITY SYSTEMS, INC.,	)	
a Delaware Corporation, INTERNET	)	
SECURITY SYSTEMS, INC., a Georgia	)	
Corporation, and SYMANTEC	)	
CORPORATION, a Delaware Corporation,	)	
	)	
Defendants and	)	
Counterclaim-Plaintiffs.	)	

**SECOND SUPPLEMENTAL RESPONSES AND OBJECTIONS OF  
ISS-GA AND ISS-DE TO SRI'S INTERROGATORY NO. 6**

Pursuant to Federal Rules of Civil Procedure 26 and 33, Defendants Internet Security Systems, Inc. ("ISS-GA"), a Georgia corporation, and Internet Security Systems, Inc. ("ISS-DE"), a Delaware corporation, (collectively, "ISS") supplement their responses to Plaintiff SRI International, Inc.'s ("SRI's") Interrogatory No. 6.

**GENERAL RESPONSES**

1. ISS's responses are made to the best of ISS's present knowledge, information and belief. ISS's responses are subject to amendment and supplementation should future investigation indicate that amendment or supplementation is necessary. ISS undertakes no obligation, however, to supplement or amend these responses other than as required by the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the District of Delaware.

2. ISS's responses are made according to information currently in ISS's possession, custody and control.

3. ISS reserves all objections or other questions as to the competency, relevance, materiality, privilege or admissibility of any information, document or thing produced in response to SRI's Interrogatories as evidence in any subsequent proceeding or trial in this or any other action for any purpose whatsoever.

4. ISS reserves the right to object on any ground at any time to additional interrogatories that SRI may propound involving or relating to the same subject matter as SRI's Interrogatories.

#### **GENERAL OBJECTIONS**

ISS incorporates their Objections contained in their Responses and Supplemental Responses to SRI's First Set of Interrogatories. The applicable objections are incorporated into each of the responses that follow. The stating of a specific objection or response shall not be construed as a waiver of ISS's general objections.

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6

INTERROGATORY NO.6:

If you contend that any claim of any of the Patents-in-Suit is invalid, identify the specific statutory bases for the invalidity (e.g., 35 U.S.C. § 102(a)), the factual bases for that contention, any allegedly invalidating prior art or publications, where each element of the claim is found in the prior art or publications, and the three people most knowledgeable about the factual bases for your contention. Your response may take the form of a claim chart.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6

ISS objects to Interrogatory No. 6 to the extent that it requests the "three people most knowledgeable about the factual bases for your contentions." This portion of the interrogatory seeks a premature identification of expert witnesses upon which ISS intends to rely. ISS further objects that this Interrogatory is overbroad to the extent that it requests information regarding claims that SRI has not asserted against ISS in this litigation. SRI has accused ISS of infringing claims 1-6 and 12-17 of the '203 patent and claims 1-6 and 13-18 of the '615 patent.

Accordingly, ISS will address those claims. Because SRI has refused to designate asserted claims for the '212 and '338 patents, ISS will address all claims of those patents. ISS refers to these claims as the "claims at issue". ISS believes that any attempt by SRI to later try to assert additional claims against ISS would be highly prejudicial to ISS, and ISS reserves the right to supplement or modify these responses in such an event.

Moreover, despite repeated requests, SRI has not provided specific contentions regarding the conception date(s) for the alleged "inventions" claimed in the patents-in-suit in response to ISS's Interrogatory No. 7. SRI's response that the subject matter of the asserted patents was conceived "no later than" the filing date of the patent application from which those patents claim

priority provides no information at all concerning conception. Similarly, SRI's attempt to rely on Rule 33(d) fails to provide alleged conception and reduction to practice dates because not only does SRI point to 38 ranges of documents, it fails to separately identify which documents it relies on for conception, which documents relate to diligence and which documents relate to a reduction to practice. To the extent that SRI has responded to Symantec's interrogatory, SRI has provided an approximately one year date range for conception of the '338, '203, and '615 patents, and an approximately two year date range for conception of the '212 patent. SRI has prejudiced ISS through its failure to provide the date(s) of conception and reduction-to-practice for each alleged "invention".

Consequently, the patentability of the claims-at-issue must be assessed in light of the state of the relevant art as of the filing date of the original application from which the patents issued. ISS intends to present evidence at trial that establishes and broadly illustrates the state of the art in intrusion detection and network monitoring as of November 9, 1998. ISS may rely upon publications, patents, percipient and expert testimony, and/or contemporaneous and predecessor products to reveal the state of such art at that time (or as of any earlier date if plaintiff offers legally adequate proof of an earlier date of invention).

The information provided in ISS's response is preliminary in nature and subject to modification and supplementation. ISS has only recently started to receive and review documents produced by SRI relating to the work that led to the patents-in-suit and certain prior art systems and references. Moreover, ISS continues to develop and refine its understanding of the state of the art as additional relevant information is acquired during the course of ongoing discovery. In addition, the complete scope of available prior art will not be known until the Court has construed the claims of the patents-in-suit. Ongoing discovery efforts may identify

additional prior art references or embodiments that are relevant to the invalidity of the claims-in-suit. ISS will supplement this response in a timely manner upon receipt of sufficient information relating to such additional prior art references or embodiments.

The Court's Scheduling Order specifies that "on January 20, 2006, the parties shall exchange lists of those claim terms that they believe need construction and their proposed claim construction of those terms" and that the "parties shall agree upon and file the Joint Claim Construction Statement on February 17, 2006, with the claim chart separately docketed." Thus, ISS has not been provided with any understanding of SRI's proposed claim constructions, and therefore is unable to determine how SRI's proposed claim construction informs the anticipation and obviousness contentions disclosed herein. Accordingly, ISS provides broad-based invalidity contentions that would include a claim scope SRI would have to assert in order to make an infringement argument against the accused ISS products. ISS reserves the right to supplement and modify its invalidity contentions under 35 U.S.C. §§ 102 and 103 subject to the claim constructions advanced by SRI. ISS further reserves the right to supplement and modify these contentions once the Court has construed the claims of the patents-in-suit.

The accompanying prior art claim charts, attached hereto as Exhibits 1-23, reflect ISS's current understanding of the primary prior art references and embodiments upon which it intends to rely to establish anticipation of the claims-in-suit under 35 U.S.C. § 102 or obviousness under 35 U.S.C. § 103. To the extent that a particular prior art reference or embodiment does not alone anticipate all the limitations of one of the claims-in-suit as ultimately construed by the court, ISS reserves the right to combine the references and/or embodiments disclosed herein with other references and/or embodiments that may complement any such reference or embodiment, to the

extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

Moreover, due to the magnitude of the prior art references that invalidate the claims at issue, as well as SRI's failure to provide conception and reduction-to-practice dates, ISS cannot possibly list every combination of art that renders those claims invalid under 35 U.S.C. § 103 and reserves the right to present different combinations of references and/or embodiments, to the extent that one skilled in the art at the relevant point in time would have had motivation to create such a combination.

#### **Relevant Prior Art References Identified To Date**

The knowledge of one skilled in the art as of Nov. 9, 1998 would have been informed by access to and appreciation of at least the following practices, publications, patents and publicly available technologies, products and systems. ISS intends to rely upon these and similar references to establish the state of the intrusion detection, network monitoring, and related arts on prior to November 9, 1998, and to establish that the claims-in-suit were anticipated under 35 U.S.C. § 102 or would have been obvious under 35 U.S.C. § 103 as of November 9, 1998:

- All prior art of record in the file history of the patents-in-suit; or identified in the specification of the patents-in-suit;
- All prior art references identified in Exhibits 1-23 attached hereto; and
- All prior art references produced to SRI.

#### **Additional Technologies, Products and Systems**

- Argus
- Arpwatch

- ASIM (Automated Security Incident Measurement)
- Berkeley Packet Filter
- Borderguard
- Bro
- Cabletron's Spectrum
- CIDF (Common Intrusion Detection Framework)
- Computer Associates Unicenter TNG
- CSM (Cooperating Security Managers)
- DIDS (Distributed Intrusion Detection System)
- EMERALD
- FireWall-1
- GridS (Graph based Intrusion Detection System)
- Harris Corporation Stake Out
- Haystack
- HP OpenView, Network Node Manager, and NetMetrix
- IDES
- Internet standards
- IP Filter
- ISM (Internetwork Security Manager)
- Ji-Nao
- Libcap
- MIDAS (Multics Intrusion Detection and Alerting System)
- NADIR (Network Anomaly Detection and Intrusion Reporter)

- NetRanger
- NFR (Network Flight Recorder)
- NIDES
- NIDX
- NSM (Network Security Monitor)
- Raxco AUDIT
- Stalker, NetStalker and WebStalker
- Sun Network Management System (Solstice Site Manager, Solstice Domain Manager, Solstice Enterprise Manager, and Sun Net Manager)
- Tcpdump
- TCP Wrapper
- TIS Firewall Toolkit
- Tivoli Enterprise Manager
- Wisdom & Sense

#### **PRIOR ART REFERENCES THAT INVALIDATE THE CLAIMS-AT-ISSUE**

The prior art invalidates the claims at issue under 35 U.S.C. §102 and/or 103, as set forth in detail in the representative charts attached as Exhibits 1-22 to this supplemental response. The cover page of each chart provides citations to referenced prior art, as well as citations to related prior art disclosures. These invalidity charts include:

- Exhibit 1: SRI's Emerald -- NISSC (October 9, 1997)
- Exhibit 2: SRI's Emerald -- CMAD Workshop, Monterey, 12-14 November 1996
- Exhibit 3: SRI's Emerald -- Conceptual Overview
- Exhibit 4: SRI's Emerald -- Conceptual Design and Planning

- Exhibit 5: SRI's Emerald -- *Live Traffic Analysis of TCP/IP Gateways*
- Exhibit 6: SRI's Nides/Network Nides
- Exhibit 7: Jinao
- Exhibit 8: NSM
- Exhibit 9: DIDS
- Exhibit 10: ISM
- Exhibit 11: GRIDS
- Exhibit 12: NetRanger
- Exhibit 13: RealSecure
- Exhibit 14: Network Flight Recorder
- Exhibit 15: NetStalker and HP OpenView
- Exhibit 16: HP OpenView and internet standards
- Exhibit 17: Network Level Intrusion Detection
- Exhibit 18: U.S. Patent No. 5,825,750
- Exhibit 19: Fault Detection in an Ethernet Network via anomaly detectors
- Exhibit 20: Stake Out
- Exhibit 21: Emerald 1997, NSM and NIDES 1994
- Exhibit 22: AIS: Automated Information System
- Exhibit 23: Summary chart of other relevant art

**THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112**

The claims-at-issue are also invalid under 35 U.S.C. § 112 for failure to satisfy the best mode requirement. SRI submitted source code in an Appendix to the patents-in-suit. A preliminary examination of that code indicates that it is not a complete program and could not

compile and run. The Appendix appears to lack configuration files that would relate specifically to network traffic data or analysis. The code also does not have code for a resolver. On information and belief, ISS believes discovery will show that SRI had a more complete set of source code by the time it filed U.S. Patent Application No. 09/188,739 and withheld much of that code from the Patent Office. That withheld code reflected the inventor's best mode of practicing the claims at issue.

ISS's contentions regarding invalidity for failure to satisfy the enablement, written description and definiteness requirements of 35 U.S.C. § 112 are premature before claim construction. ISS reserves the right to supplement this response.

#### **SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6**

Subject to and without waiving its objections, ISS further provides the following.

#### **PRIOR ART REFERENCES THAT INVALIDATE THE CLAIMS-AT-ISSUE**

In Exhibit A attached hereto, ISS provides updated cover pages for the invalidity charts attached as Exhibits 1-22 to ISS's Supplemental Response To Interrogatory No. 6.

#### **THE CLAIMS-AT-ISSUE ARE INVALID PURSUANT TO 35 U.S.C. § 112**

Discovery has confirmed that SRI failed to disclose the best known mode of practicing the Asserted Claims at the time it filed the patent application from which all patents-in-suit claim priority. The material in SRI's escrowed computer establishes that SRI had source code existing at the time of filing that (1) pertained to SRI's best known mode of practicing the Asserted Claims and (2) was withheld from the Appendix submitted to the Patent Office. Deposition testimony of Keith Skinner, Ulf Linqvist, Martin Fong, Alfonso Valdes and Phillip Porras and

SRI's responses to Symantec's Requests for Admission Nos. 51-89 further confirm SRI's failure to disclose the best mode.

Moreover, should the Asserted Claims and prior art be construed as SRI contends, those claims would be invalid under 35 U.S.C. § 112 for lack of enablement, indefiniteness and failure to meet the written description requirement. SRI has argued in response to ISS's invalidity showing that many pieces of prior art are "unenabling." See SRI's responses on CMAD, EMERALD Conceptual Overview, the Network NIDES paper, JiNao, and DIDS; *see also* Valdes testimony regarding the EMERALD NISSC 1997 paper, Valdes Tr. at pp. 552-54. The patent application is written at the level of these papers and the Appendix contains no code that is specific to network traffic analysis. In particular, much of the written description of the patents-in-suit is drawn from the EMERALD NISSC 1997 paper and figures in the patents-in-suit also appear in the CMAD, EMERALD Conceptual Overview and EMERALD NISSC 1997 paper. Therefore, if these prior art references are "unenabling", then so is the patent specification. The patent specification would also fail to meet the written description requirement.

Should the Asserted Claims and prior art be construed as SRI contends, the Asserted Claims containing the limitations of "integrating the reports of suspicious activity"; "correlating intrusion reports reflecting underlying commonalities" and "correlates activity" are indefinite, unenabled and not described. There is no mention, let alone teaching, in the written description of how to perform these method steps, nor is there anything in the appendix pertaining to integration or correlation of intrusion reports. One of skill in the art cannot understand what falls within the scope of the claim. Moreover, the named inventors did not have possession of these method steps at the time the application was filed.

Discovery and claim construction are still on-going in this case. ISS reserves the right to further supplement this response.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

Holmes J. Hawkins III  
Bradley A. Slutsky  
Natasha H. Moffitt  
KING & SPALDING LLP  
191 Peachtree Street  
Atlanta, GA 30303  
Tel: (404) 572-4600

Theresa A. Moehlman  
Bhavana Joneja  
KING & SPALDING LLP  
1185 Avenue of the Americas  
New York, New York 10036  
Tel.: (212) 556-2100

Dated: April 10, 2006  
727188 / 28434

By: /s/ David E. Moore

Richard L. Horwitz (#2246)  
David E. Moore (#3983)  
Hercules Plaza 6th Floor  
1313 N. Market Street  
Wilmington, DE 19801  
Tel: (302) 984-6000  
[rhorwitz@potteranderson.com](mailto:rhorwitz@potteranderson.com)  
[dmoore@potteranderson.com](mailto:dmoore@potteranderson.com)

*Attorneys for Defendants*  
*INTERNET SECURITY SYSTEMS, INC.,*  
*a Delaware corporation; and*  
*INTERNET SECURITY SYSTEMS, INC.,*  
*a Georgia corporation*

# EXHIBIT A

**EMERALD 1997 invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations are taken from: P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISSC October 9, 1997 (ISS 2892-2904). SRI admits this paper was published on October 9, 1997 in the Proceedings of the 20<sup>th</sup> National Information Systems Security Conference (NISSC). (SRI's response to ISS-GA's Request For Admission No. 1).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- P. Neumann, P. Porras and A. Valdes, *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (ISS 348257-348258)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (SRI 11022-11026)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 (SRI 11045-11048)
- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, December 18, 1996. (ISS 44439-44441)
- P. Porras and P. Neumann, *CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, Version 1.2 May 20, 1997, <http://www.csl.sri.com/intrusion.html> (SRI 12308-12404).

**CMAD invalidates the indicated claims under 35 U.S.C. § 102(b) and/or 103**

- All "CMAD" text citations are taken from: *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (ISS 348257-348258); This paper was handed out at the CMAD workshop. (Neumann Dep. Tr. at 85-86.)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

103

It would have been obvious to combine the disclosure of CMAD with the additional references cited herein under "103", because all of the references cited relate to extending NIDES to network-based analyses:

- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISSC October 9, 1997 (hereinafter "EMERALD 1997") (ISS 2892-2904) SRI admits this paper was published on October 9, 1997 in the Proceedings of the 20<sup>th</sup> National Information Systems Security Conference (NISSC). (SRI's response to ISS-GA's Request For Admission No. 1).
- D. Anderson, T. Frivold, and A. Valdes, *Next-Generation Intrusion Detection Expert System (NIDES): A Summary*, Computer Science Laboratory, SRI-CSL-95-07 (May 1995) (hereinafter "NIDES: A Summary") (ISS 359733-359778)

Similar disclosures and additional related information are contained in the following additional references:

- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 (SRI 11045-011048)
- P. Neumann, P. Porras and A. Valdes, *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996. (SRI 11022-11026)
- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, December 18, 1996. (ISS 44439-44441)

- P. Porras and P. Neumann, CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Version 1.2 May 20, 1997, <http://www.csl.sri.com/intrusion.html> (SRI 12308-12404)
- Proceedings of the Fourth Workshop on Future Directions in Computer Misuse and Anomaly Detection, Session Summaries, Monterey, California, November 12-14, 1996 (ISS 354559)
- CMAD IV, Computer Misuse and Anomaly Detection, Presentation Slides and Papers, Monterey, California, November 12-14, 1996 (ISS 00354560-354606)

***Emerald Conceptual Overview* invalidates the indicated claims under  
35 U.S.C. § 102(b) and/or 103**

- All "Emerald Conceptual Overview" text citations are taken from: P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, December 18, 1996, which was available on SRI's website at least as early as July 5, 1997. (ISS 44439-44441)

This paper was publicly available on December 18, 1996 (SRI's Response To ISS-GA's Request For Admission No. 3).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

**103**

It would have been obvious to combine the disclosure of *Emerald Conceptual Overview* with the additional references cited herein under "103", because all of the references cited relate to extending NIDES to network-based analyses:

- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISSC October 9, 1997 (hereinafter "*EMERALD 1997*") (ISS 2892-2904). SRI admits this paper was published on October 9, 1997 in the Proceedings of the 20<sup>th</sup> National Information Systems Security Conference (NISSC).
- D. Anderson, T. Frivold, and A. Valdes, *Next-Generation Intrusion Detection Expert System (NIDES): A Summary*, Computer Science Laboratory, SRI-CSL-95-07 (May 1995) (hereinafter "*NIDES: A Summary*") (ISS 359733-359778)

Similar disclosures and additional related information are contained in the following additional references:

- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 (SRI 11045-11048)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (SRI 11022-11026)

- P. Neumann, P. Porras and A. Valdes, *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996. (ISS 348257-348258)
- P. Porras and P. Neumann, CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Version 1.2 May 20, 1997, <http://www.csl.sri.com/intrusion.html> (SRI 12308-12404)

Article Marked as "Confidential - Subject To Protective Order" by SRI

**Conceptual Design and Planning for Emerald: Event Monitoring Enabling Responses To Anomalous Live Disturbances, Version 1.2, 20 May 1997**  
**Invalidate the Indicated Claims Under 35 U.S.C. § 102(b) and/or § 103**

All Citations are to:

- P. Porras and P. Neumann, "Conceptual Design and Planning for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Version 1.2 20 May 1997. (SRI 12308-12404) ("Emerald Conceptual Design"). The cover page of this paper indicates that it was available on <http://www.csl.sri.com/intrusion.html>. Moreover, the paper P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," 20<sup>th</sup> NISSC - October 9, 1997 (ISS 28352), indicates this paper was available for download via <http://www.csl.sri.com/intrusion.html>. Despite the public availability of this document, SRI has produced it as confidential. Therefore, ISS-GA has indicated this confidential marking on this chart.

Mr. Porras testified this was a living document that was continually updated. (Porras Rule 30(b)(6) Deposition (March 30, 2006) at 98). Early versions of this paper provide a similar disclosure and may be found at SRI 012308-404 (printed on May 16, 1997); SRI 154894-932 (printed on February 2, 1997).

SRI 154809-154812 indicates the report was on available on SRI's publicly available website at <http://www.csl.sri.com/intrusion.html> on or about March-April 1997, when the Second Quarterly Report was provided to DARPA. SRI105389-609 at SRI 105590 indicates the report was available at <ftp://ftp.csl.sri.com/pub/emerald-concepts1.ps> at least as early as February 5, 1997. Concepts.ps is the file name associated with "Conceptual Design and Planning for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," as indicated in SRI 034454-63.

The text included herein are merely representative samples of the disclosure in the assert reference. ISS reserves the right to supplement these disclosures.

103

It would have been obvious to combine the disclosure of Emerald Conceptual Design with the references cited below under "other prior art" because all references relate to intrusion detection analysis and both JINAO and EMERALD draw from the NIDES project at SRL.

Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 ("JINAO") (ISS 27334-27374)

Y. Frank Jou and S. Felix Wu, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, IDS Program Review, SRL, July 1997, ("JINAO Slides") (ISS 27377-27406)

Similar disclosures and additional information are referenced in the cover pages to the charts for the other EMERALD papers.

***Live Traffic Analysis* invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations are taken from: P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, <http://www.sdl.sri.com/projects/emerald/live-traffic.html>, Internet Society's Networks and Distributed Systems Security Symposium, Nov. 10, 1997 (ISS 28365-28384)

A postscript version of this paper was publicly available on SRI's website as of August 1, 1997 (Porras Rule 30(b)(6) deposition (March 30, 2006) at p. 111) and a html version of this paper was publicly available on SRI's website as of August 25, 1997 (Porras Rule 30(b)(6) (March 30, 2006) deposition at pp. 120-122).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways, Networks and Distributed Systems Security Symposium*, March 1998 (ISS 359692-359712)
- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISSC October 9, 1997 (ISS 2892-2904)
- P. Neumann, P. Porras and A. Valdes, *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (ISS 348257-348258)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for CMAD Workshop, Monterey, 12-14 November 1996 (SRI 11022-11026)
- *Analysis and Response for Intrusion Detection in Large Networks*, Summary for Intrusion Detection Workshop, Santa Cruz, 26-28 August 1996 (SRI 11045-11048)

- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, December 18, 1996 (ISS 44439-44441)
- P. Porras and P. Neumann, *CONCEPTUAL DESIGN AND PLANNING for EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, Version 1.2 May 20, 1997, <http://www.csl.sri.com/futrusion.html> (SRI 12308-12404)

***Next-Generation Intrusion Detection Expert System (NIDES): A Summary invalidates the indicated claims under 35 U.S.C. § 102(b)***

All text citations are taken from: D. Anderson, T. Frivold, and A. Valdes, *Next-generation Intrusion Detection Expert System (NIDES) A Summary*, Computer Science Laboratory, SRI-CSL-95-07, May 1995 (ISS 359733-359778)

This paper was indexed on SRI's website as available by request at least as early as July 5, 1997 (SYM\_P\_0078552-61; Exhibit 15 to the Porras Rule 30(b)(6) Deposition on March 30, 2006); see also SRJE 0053394-95 (showing distribution of the paper in December 1996).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.G. Neumann, and C. Jalali, "IDES: A Progress Report," in Proceedings of the 6th Annual Computer Security Applications Conference, 1990 (ISS 27834-27846)
- T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, H.S. Javitz, A. Valdes, and P.G. Neumann, "A Real-Time Intrusion-Detection Expert System (IDES)," Interim Progress Report, Project 6784, SRI International, May 16, 1990<sup>\*</sup> (ISS 355143-355280)
- T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey, "A Real-Time Intrusion Detection Expert System (IDES) – Final Technical Report," Tech. Rep., SRI Computer Science Laboratory, SRI International, Menlo Park, CA, Feb. 28, 1992 (ISS 27669-27833)

**Ji-Nao invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations for "Ji-Nao" are taken from: Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997, posted on the MCNC website as early as October 1997. (ISS 27334-27374)

All text citations for "Ji-Nao slides" are taken from: Y. Frank Jou and S. Felix Wu, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, IDS Program Review, SRI, July 1997, posted on the MCNC website as early as October 1997. (ISS 27377-27406)

Mr. Jou testified that he put these materials on the MCNC website at least as early as April 25, 1997 and distributed an email to the DARPA intrusion detection community to inform them of the availability of the material. (Jou Dep. Tr. at pp. 75-77; Exhibit J17 (SRIE 0399295)).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- Shyh-tsun F. Wu et al., *Intrusion Detection for Link-State Routing Protocols*, December 2, 1996 (ISS 27408-27416)
- MCNC Internet Archive pages, including Project Update Viewgraph slides at SRI, July 1997 (ISS 00592400-00592429)
- MCNC Internet Archive pages, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, April 1997 (ISS 00592355-00592356)
- Diheng Qu et al., *Statistical Anomaly Detection for Link-State Routing Protocols*, in Sixth International Conference on Network Protocol (ICNP '98) October 1998 (ISS 27462-27470)

**NSM invalidates the indicated claims under 35 U.S.C. § 102(b)**

Cited text is taken from L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood, D. Wolber, "A Network Security Monitor," *Proc. 1990 Symposium on Research in Security and Privacy*, pp. 296-304, May 1990 (ISS 4149-4157). SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 12).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," *IEEE Network*, Vol. 8 No. 3, pp. 26-41, May/June 1994 (ISS 23541-23557)
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "A Method to Detect Intrusive Activity in a Networked Environment," *Proc. 14th National Computer Security Conference*, pp. 362-371, Oct. 1991 (ISS 23957-23967); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 14).
- L.T. Heberlein, "Towards Detecting Intrusions in a Networked Environment," Technical Report CSE-91-23, Division of Computer Science, UC Davis, June 1991 (ISS 23866-23924)
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, G. Dias, D. Mansur, "Towards Detecting Intrusions in a Networked Environment," *Proc. 14th Department of Energy Computer Security Group Conference*, pp. 17.47-17.65, May 1991 (ISS 23846-23865)
- L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood, "Network Attacks and an Ethernet-based Network Security Monitor," *Proc. 13th Department of Energy Computer Security Group Conference*, pp. 14.1-14.13, May 1990 (ISS 25306-25318)
- L. Todd Heberlein, Network Security Monitor Final Report, February 1995 (ISS 4149-4157)

### DIDS invalidates the indicated claims under 35 U.S.C. § 102(b)

All citations in "DIDS February 1991" are taken from: Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and A Proposed Distributed IDS Architecture" (February 1991) (ISS 24900-24917)

All citations in "DIDS October 1991" are taken from: S.R. Snapp, J. Brentano, G.V. Dias, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, (with S.E. Smaha, T. Grance, D.M. Teal, D.L. Mansur), "DIDS -- Motivation, Architecture, and an Early Prototype," Proc. 14th National Computer Security Conference, Washington, DC, Oct. 1991, pp. 167-176 (ISS 4080-4089). SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 19).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, L.T. Heberlein, C.L. Ho, K.N. Levitt, B. Mukherjee, (with T. Grance D.L. Mansur, K.L. Pon, S.E. Smaha), "A System for Distributed Intrusion Detection," COMPCON Spring '91. Digest of Papers. San Francisco, CA, 25 Feb.-1 March 1991, pp. 170-176 (ISS 23817-23823)
- J. Brentano, S.R. Snapp, G.V. Dias, T.L. Goan, L.T. Heberlein, C.L. Ho, K.N. Levitt, B. Mukherjee, (with S.E. Smaha), "An Architecture for a Distributed Intrusion Detection System," Proc. of the 14th Department of Energy Computer Security Group Conference, May 1991, pp.(17)25-(17)45 (ISS 23824-23845)
- Steve Snapp, "Signature analysis and communication issues in a distributed intrusion detection system," M.S. Thesis, Division of Computer Science, University of California, Davis, August 1991 (ISS 03336-03378)
- Steven R. Snapp, Stephen E. Smaha, Daniel M. Teal, Tim Grance, "The DIDS (Distributed Intrusion Detection System) Prototype," Proceedings of the Summer 1992 USENIX Conference, June 8-12, 1992 (SYM\_P\_0501723-SYM\_P\_0501736)
- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection", IEEE Network, May-June 1994, Vol. 8, No. 3, p. 26-41 (ISS 23541-23557)

***ISM and DIDS invalidate the indicated claims under 35 U.S.C. § 102(b) or 103.***

All text citations are taken from:

- *L.T. Heberlein, B. Mukherjee, K.N. Levitt, Internetwork Security Monitor*, Proc. of the 15th National Computer Security Conference, October 1992, pp. 262-271 ("ISM") (ISS 23346-23356); SRI admits this paper was published before November 9, 1997 (SRI's Response to Symantec's Request for Admission No. 48).
- S.R. Snapp, J. Brentano, G.V. Dias, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, (with S.E. Smaha, T. Grance, D.M. Teal, D.L. Mansur), "DIDS - Motivation, Architecture, and an Early Prototype" Proc. 14th National Computer Security Conference, Washington, DC, Oct. 1991, pp. 167-176 ("DIDS") (ISS 4080-89); SRI admits this paper was published before November 9, 1997 (SRI's Response to Symantec's Request for Admission No. 19).

The text included herein are merely representative samples of the disclosure in the asserted reference. Symantec reserves the right to supplement these disclosures.

**102(b)**

*ISM* invalidates the indicated claims under § 102(b). Additionally, *ISM* and *DIDS* constitute a single disclosure for purposes of 35 USC § 102(b) because *ISM* incorporates-by-reference the text of *DIDS*. *ISM* cites to *DIDS*. See *ISM* at 263, 264, 271. Furthermore, *ISM* explicitly states that *ISM* is an extension of *DIDS*:

Primarily, the *ISM* extends the Distributed Intrusion Detection System (*DIDS*) (see [Sna91]) into arbitrarily wide networks.

*ISM* at 264.

**103**

In the alternative, *ISM* in combination with *DIDS* renders the indicated claims invalid due to obviousness under 35 USC § 103. The citations above provide a motivation to combine *ISM* and *DIDS* in order to extend *DIDS* to larger networks.

### GrIDS invalidates the indicated claims under 35 U.S.C. § 102(b)

Text citations to "GrIDS 1996" are taken from: Chen, S.S., et al. "GrIDS - A Graph Based Intrusion Detection System For Large Networks" in 19th National Information Systems Security Conference, 1996 (ISS 03423-03432)

Text citations to "GrIDS 1997" are taken from: Steven Cheung, Rick Crawford, Mark Dilger, Jeremy Frank, Jim Hoagland, Karl Levitt, Stuart Staniford-Chen, Raymond Yip, Dan Zerkle, "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical report, UC Davis Department of Computer Science, Davis California (May 14, 1997) (ISS 340942-341017). This document was publicly available on the web at least as early as July 19, 1997 (Graph-based Intrusion Detection System (GRIDS) Home Page, webpage archived July 19, 1997 (ISS 340935-340936)).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- GrIDS Requirements Document, webpage archived December 14, 1996 (ISS 340937)
- GrIDS Outline Design Document, webpage archived December 14, 1996 (ISS 340938-340941)
- Graph-Based Intrusion Detection System Presentation, PI Meeting, Savannah, GA, Feb 25-27, 1997 (ISS 341018-341025)

**NetRanger invalidates the indicated claims under 35 U.S.C. § 102(b)**

"NetRanger Publication" is based upon the NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 (ISS 340607-340933)

"NetRanger Product" is based upon the NetRanger software versions 2.0 and earlier. The capabilities of this software are demonstrated in:

- NetRanger Real-Time Network Intrusion Detection Performance and Security Test, SPOCK Consortium Demonstration Report, Department of Defense Doc. No. 010511, including Appendices A, B and C, April 30, 1997 (ISS 44725-44950)
- NetRanger SQL queries, 5/28/1997 (ISS 359330-359351)
- NetRanger training slide presentations, 4/1997 (ISS 354607-354724)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- NetRanger User's Guide Version 2.1.1, Cisco Systems, Inc., 1998 (ISS 3000-3335)
- Release Notes for NetRanger 2.1.1, Cisco Systems, Inc., 1998 (ISS 2905-2933)
- Networkers Active Audit - Scanning, and Intrusion Detection, Cisco US Networkers '98, 6/16/1998. (ISS 2980-2999)
- PC Week, "NetRanger keeps watch over security leaks," September 1, 1997 (ISS 28277-28280)
- "WheelGroup Releases NetRanger Version 2.0," WheelGroup press release, Aug. 25, 1997 (ISS 44716-44717)
- "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger Intrusion Detection System." WheelGroup press release, July 8, 1997 (ISS 44718-44719)
- WheelGroup Press Release Summary (ISS 44714-44715)
- NetRanger User's Guide 1.2.2, WheelGroup Corporation, 1997 (ISS 341260-341512)

- NetRanger User's Guide 1.2, WheelGroup Corporation, 1997 (ISS 31240-31469)
- Product Security Assessment of the NetRanger Intrusion Detection Management System Version 1.1, The Air Force Information Warfare Center/Engineering Analysis Directorate (AFIWC/EA), 2/1997 (ISS 341513-341552)
- NetRanger High-Level Overview, Version 1.1, WheelGroup Corporation, 11/1996 (ISS 23695-23711)
- NetRanger User's Guide, WheelGroup Corporation, 1996 (ISS 31069-31239)
- Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 (ISS 30066-30305)

### RealSecure invalidates the indicated claims under 35 U.S.C. § 102(b)

“RealSecure” invalidity is shown both by the publications listed below and by the RealSecure product they identify and describe. RealSecure was on-sale more than a year before SRI’s priority date.

- RealSecure 1.2.2: User Guide and Reference Manual (9/11/97) (ISS 312059-312076, ISS 312114-312128 and ISS 312134-312157)
- RealSecure 1.2: User Guide and Reference Manual (1997) (ISS 25469-25566)
- RealSecure 1.1: User Guide and Reference Manual (3/97) (ISS 25387-25463)
- RealSecure 1.0: User Guide and Reference Manual (1996) (ISS 354437-354465)
- *More About RealSecure: General Description and Comparison to Existing Systems* (available at least as early as 07/21/1997, see archive.org) (ISS 357169-357178)
- *Frequently-Asked Questions About RealSecure* (last updated 5/30/1997, available at least as early as 07/21/1997, see archive.org) (ISS 357179-357193)
- *Real-Time Attack Recognition and Response: A Solution for Tightening Network Security* (available at least as early as 1/20/98, see archive.org) (ISS 357242-357259)
- *Frequently Asked Questions About Real-Secure* (last updated 10/21/97, available at least as early as 1/20/98, see archive.org) (ISS 357217-357227)
- RealSecure Press Releases (ISS 357164-357165, ISS 357262 and ISS 357263)
- RealSecure Release Dates Table (ISS 358384)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Additional information is contained in:

- R. Power and R. Farrow, *Detecting Network Intruders*, Network Magazine, pp. 137-38, October 1997 (ISS 341748-341751)

**The Network Flight Recorder System invalidates the indicated claims under 35 U.S.C. § 102(b) and/or § 103**

All text citations for "Network Flight Recorder" are taken from: "Implementing A Generalized Tool For Network Monitoring," by Ranum et al., Proceedings of the Eleventh Systems Administration Conference (LISA '97); San Diego, CA, Oct. 1997 (ISS 24542-24550)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

**103**

It would have been obvious to combine the disclosure of Network Flight Recorder ("NFR") with the additional references cited herein under "other prior art" because all of the references cited relate to network-based intrusion detection analyses.

*Next-generation Intrusion Detection Expert System (NIDES) A Summary*, Computer Science Laboratory, SRI-CSL-95-07, May 1995 ("NIDES"); (ISS 359733-359778)

Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network*, Technical Report CDRL A005, DARPA Order No. E296, Dept. of Computer Science North Carolina State University, April 1997 ("JINAO") (ISS 357064-357136)

Y. Frank Jou and S. Felix Wu, *Scalable Intrusion Detection for the Emerging Network Infrastructure*, IDS Program Review, SRI, July 1997, ("JINAO Slides") (ISS 27334-27374)

P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISCC October 9, 1997 ("EMERALD") (ISS 2892-2904)

RealSecure 1.1 - User Guide and Reference Manual (3/97) (ISS 25387-25463)

Similar disclosures and additional related information are contained in the following additional references:

- NFR Beta Handbook, November 1997 (ISS 359157-359244)

- NFR User Guide, Version 1.1, November 1997 (ISS 359943-360013)
- NFR Version 1.0beta2 Source Code (ISS 360127-362159)
- Frequently Asked Questions/Troubleshooting Guide for NFR (ISS 359153-359156)
- Other NFR Version Obeta2 Materials (ISS 359140-359152)
- NFR Version 2.0 Library, October 5, 1998 (ISS 359483)
- NFR Version 2.0 Getting Started Guide (ISS 359484-359496)
- NFR Version 2.0 User's Guide (IS 359497-359543)
- NFR Version 2.0 Advanced User's Guide (ISS 359544-359588)
- NFR Version 2.0 Reference Document (ISS 359589-359676)
- NFR Version 2.0 Glossary (ISS 359677-359678)
- R. Power and R. Farrow, "Detecting Network Intruders," Network Magazine, October 1997 pp. 137-138 (ISS 341748-341751)

**NetStalker and HP Openview invalidate the indicated claims under 35 U.S.C. § 102(b) and/or 103**

All Citations are to:

- NetStalker, Installation and User's Guide, Version 1.0.2, (May 1996 [1.0.2] (ISS 30989-31068))
- HP OpenView for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and '97 for Windows NT, 3Com, October 1997 (ISS 26617-26771)
- RFC 1157, A Simple Network Management Protocol (SNMP), May 1990 (ISS 34897-349019); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 44).
- RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990 (ISS 34886-348905); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 45).
- RFC 1271, Remote Network Monitoring Management Information Base, November 1991 (ISS 349177-349249); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 47).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

NetStalker and HP OpenView were both on-sale prior to November 9, 1997. They worked together through the use of SNMP traps. Therefore, the use of the two together act as § 102(b) art. The manuals describe their operation.

Moreover, HP OpenView for Windows User Guide, Oct. 1997 and RFCs 1155, 1157, 1213 and 1271 constitute a single disclosure for purposes of 35 USC § 102(b) because HP OpenView for Windows User Guide, Oct. 1997 incorporates-by-reference the text of these RFCs. HP OpenView for Windows User Guide, Oct. 1997 devotes several chapters to use of SNMP: see, e.g., Chap. 5 "Managing SNMP Network Devices," and Chap. 7 "Custom Controls." HP OpenView for Windows User Guide, Oct. 1997 specifically references and relies upon the information in these RFCs:

"The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB).... The SNMP Manager supports all Internet MIB-II variables and can be extended to support other MIBs. (5-1)  
"MIB-2 dependent MIBs, such as rmon, would be added to the structure under the MIB-2 group" (5-19)  
"OpenView provides the MIBs for both MIB-2 (RFC1213) and rmon (RFC1271)" (5-20)

In the alternative, the NetStalker manual in combination with HP OpenView for Windows User Guide, Oct. 1997 and RFCs 1155, 1157, 1213 and 1271 renders the patents invalid due to obviousness under 35 USC § 103. The referenced use of SNMP traps and the referenced citations, where the text is incorporated by reference, provide motivation to combine in order to make and improve the network traffic monitoring claimed in the patents-in-suit.

Similar disclosures and additional information may be found in the following additional references:

- HP OpenView for Windows Workgroup Node Manager User Guide, Transcend Management Software version 6.0 for Windows, 3Com, January 1997 (ISS 26772-26885)
- M. Siegl, and G. Trausmuth, *Hierarchical Network Management - A Concept and its Prototype in SNMPv2*, 1996 (ISS 348739-348748)
- HP SNMP/XL User's Guide, HP 3000 MPE/iX Computer Systems Edition 5, Hewlett Packard, April 1994 (ISS 348749-348837)
- RFC 1441, Introduction to version 2 of the Internet-standard Network Management Framework, April 1993 (ISS 349083-349095)
- RFC 1757, Remote Network Management Information Base, February 1995 (ISS 349096-349176)
- RFC 1451, Manager-to-Manager Management Information Base, April 1993 (ISS 349250-349284)
- Mark Miller, Managing Internetworks with SNMP, Second Edition, 1997 (ISS 358409-359136)
- NetStalker Product Information (available as early as Nov. 5, 1996, see archive.org) (ISS 359727-359732)
- R. Power & R. Farrow, "Detecting Network Intruders," Network Magazine, October 1997, pp. 137-138 (ISS 341748-341751)

## HP OpenView and the Internet standards invalidate the indicated claims under 35 U.S.C. § 102(b) and/or 103

All citations are to:

- HP OpenView for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and '97 for Windows NT, 3Com, October 1997 (ISS 26617-26771)
- RFC 1157, A Simple Network Management Protocol (SNMP), May 1990 (ISS 348987-349019); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 44)
- RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990 (ISS 348886-348905); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 45).
- RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March 1991 (ISS 349020-349082); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 46).
- RFC 1271, Remote Network Monitoring Management Information Base, November 1991 (ISS 349177-349249); SRI admits this paper was published before November 7, 1997 (SRI's Response to Symantec's Request For Admission No. 47).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

HP OpenView for Windows User Guide, Oct. 1997 and RFCs 1155, 1157, 1213 and 1271 constitute a single disclosure for purposes of 35 USC § 102(b) because HP OpenView for Windows User Guide, Oct. 1997 incorporates-by-reference the text of these RFCs. HP OpenView for Windows User Guide, Oct. 1997 devotes several chapters to use of SNMP: see, e.g., Chap. 5 "Managing SNMP Network Devices," and Chap. 7 "Custom Controls." HP OpenView for Windows User Guide, Oct. 1997 specifically references and relies upon the information in these RFCs:

"The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB).... The SNMP Manager supports all Internet MIB-II variables and can be extended to support other MIBs. (5-1)

"MIB-2 dependent MIBs, such as rmon, would be added to the structure under the MIB-2 group" (5-19)  
"OpenView provides the MIBs for both MIB-2 (RFC1213) and rmon (RFC1271)" (5-20)

In the alternative, HP OpenView for Windows User Guide, Oct. 1997 in combination with RFCs 1155, 1157, 1213 and 1271 renders the patents invalid due to obviousness under 35 USC § 103. The citations above provide a motivation to combine in order to make and improve the network traffic monitoring claimed in the patents-in-suit.

Similar disclosures and additional related information are contained in the following additional references:

- HP OpenView for Windows Workgroup Node Manager User Guide, Transcend Management Software version 6.0 for Windows, 3Com, January 1997 (ISS 26772-26885)
- M. Siegl, and G. Trausmuth, *Hierarchical Network Management – A Concept and its Prototype in SNMPv2*, 1996 (ISS 348739-348748)
- HP SNMP/XL User's Guide, HP 3000 MPE/XX Computer Systems Edition 5, Hewlett Packard, April 1994 (ISS 348749-348837)
- RFC 1441, Introduction to version 2 of the Internet-standard Network Management Framework, April 1993 (ISS 349083-349095)
- RFC 1757, Remote Network Management Information Base, February 1995 (ISS 349096-349176)
- RFC 1451, Manager-to-Manager Management Information Base, April 1993 (ISS 349250-349284)
- Mark Miller, *Managing Internetworks with SNMP*, Second Edition, 1997 (ISS 358409-359136)

**“Network Level Intrusion Detection System” (August 1990) invalidates the indicated claims  
under 35 U.S.C. § 102(b)**

Cited text is taken from: Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla, “The Architecture of a Network Level Intrusion Detection System,” Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 1990 (ISS 354419-354436)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

**U.S. Pat. No. 5,825,750 (Thompson) invalidates the indicated claims under 35 U.S.C. § 102(a) and 102(e)**

All cited text is taken from: U.S. Pat. No. 5,825,750, to Horace C. Thompson, entitled "Method and apparatus for maintaining security in a packetized data communications network," filed on March 29, 1996 and issued on October 20, 1998. (ISS 360072-360081)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Additional related information is contained in:

- C. Schuba, "On The Modeling, Design and Implementation Of Firewall Technology, PhD Thesis, December 1997, pp. 87-122 (ISS 359779-359942)

***“Fault Detection in an Ethernet network via anomaly detectors” invalidates the indicated claims under 35 U.S.C. § 102(b)***

All citations are to:

Feather, Frank Edward, Ph.D., *Fault Detection in an Ethernet network via anomaly detectors*, Carnegie Mellon University, Order number 9224199, 1992 (ISS 348259-348515)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- Roy A Maxion and Frank E. Feather, *A Case Study of Ethernet Anomalies in a Distributed Computing Environment*, IEEE Transactions on Reliability, Vol. 39, No. 4, October 1990 (ISS 359274-359285)
- Frank Feather, Dan Siewiorek and Roy Maxion, *Fault Detection in an Ethernet Network Using Anomaly Signature Matching*, Computer Communication Review, SIGCOMM '93 Conference Proceedings, September 13-17, 1992 (ISS 359352-359367)

***Stake Out Network Surveillance* invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations are taken from: Harris Corporation, *Stake Out Network Surveillance White Paper* (1996) (ISS 358230-358240)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

Similar disclosures and additional related information are contained in the following additional references:

- Archived copies of Harris Corporation Web Site from <http://archive.org> (ISS 359246-359273)

***EMERALD 1997, Intrusive Activity 1991, and NIDES 1994* invalidate the indicated claims under 35 U.S.C. § 102(b) or 103.**

All text citations are taken from:

- P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20<sup>th</sup> NISSC October 9, 1997 ("Emerald 1997") (ISS 2892-2904); SRI admits this paper was published on October 9, 1997 in the Proceedings of the 20<sup>th</sup> National Information Systems Security Conference (NISSC). (SRI's response to ISS-GA's Request For Admission No. 1).
- L.T. Heberlein, B. Mukherjee, K.N. Levitt., *A Method to Detect Intrusive Activity in a Networked Environment*, Proc. 14th National Computer Security Conference, pp. 362-371, Oct. 1991 ("Intrusive Activity 1991") (ISS 23957-23967)
- H.S. Javitz and A. Valdes, *The NIDES Statistical Component Description and Justification*, Annual Report A010, SRI Project 3131, Contract N00039-92-C-0015, March 7, 1994 ("NIDES 1994") (ISS 30446-30493)

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

**102(b)**

*Emerald 1997, Intrusive Activity 1991, and NIDES 1994* constitute a single disclosure for purposes of 35 USC § 102(b) because *Emerald 1997* incorporates-by-reference the text of *Intrusive Activity 1991* and *NIDES 1994*. *Emerald 1997* cites to both articles as references, see *Emerald 1997* at 365, [7] and [9]. In addition, *Emerald 1997* explains that the statistical algorithms in *NIDES 1994* provide the foundation for the profile-based anomaly detection in *Emerald 1997*:

Requirements for an anomaly-detection system that became IDES were documented in [6]. This research led to the development of the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users [9].

See *Emerald 1997* at 359. *Emerald 1997* also directs one of skill in the art to the Network Security Monitor system for analysis of network traffic:

[T]he Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails...

See *Emerald 1997* at 364.

103

In the alternative, *Emerald 1997* in combination with *Intrusive Activity 1991* and *NIDES 1994* renders the patents invalid due to obviousness under 35 USC § 103. The citations above provide a motivation to combine in order to make and improve the statistical profiles and network traffic monitoring claimed in the patents-in-suit.

**Automated Information System - AIS  
invalidates the indicated claims under 35 U.S.C. § 102(b)**

All text citations are taken from: William Huntman, "Automated Information System—(AIS) Alarm System," Proc. Of the 20th National Systems Security Conference (October 1997) (SYM\_P\_0526260-SYM\_P\_0526260).

The text included herein are merely representative samples of the disclosure in the asserted reference. ISS reserves the right to supplement these disclosures.

# **EXHIBIT**

# **M**

**REDACTED**